

# 多云流量调度和接入在虎 牙的落地实践

中间件团队 / 周健

# 分享内容

---

1

云上流量接入现状

2

标准化，统一计费

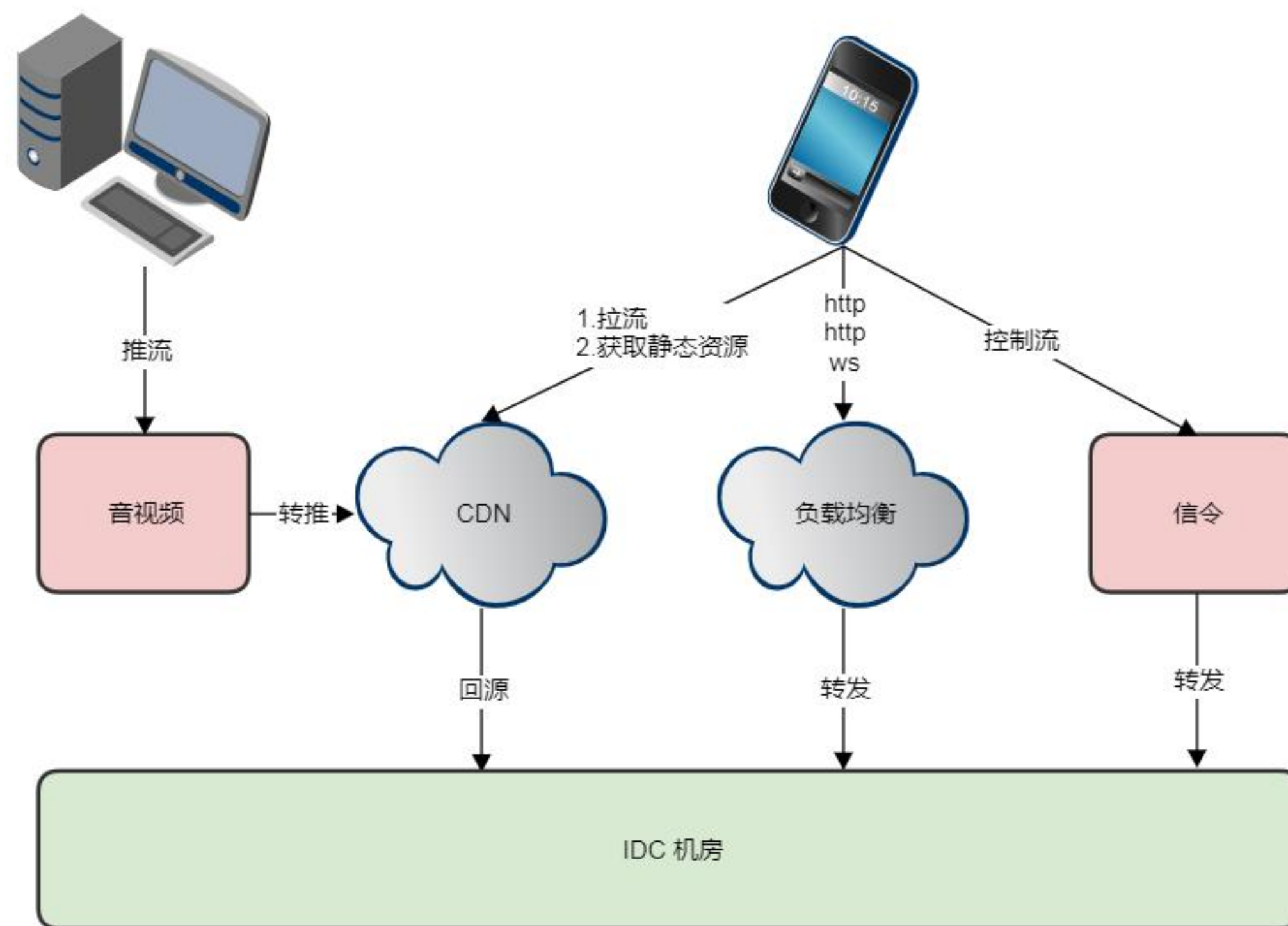
3

建立流量调度体系

4

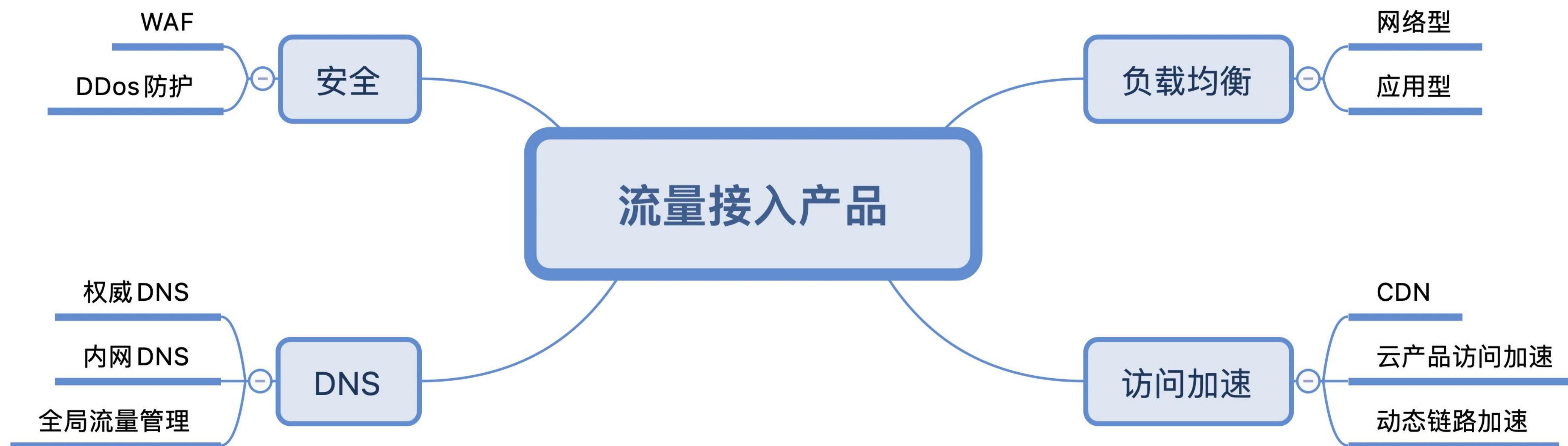
多云收益最大化

# 虎牙流量接入的现状





# 流量接入产品多样



# 多云之间差异

## 监控

粒度，统计口径不一致  
指标差异  
监控延迟



## 管理API

缺少统一API规范  
调用频率限制  
延迟



## 计费模式

规格 or LCU



# 接入成本高昂，难以控制



# 网络故障是常态

| 分类  | 原因     | 影响时间      | 影响范围               | 频率     |
|-----|--------|-----------|--------------------|--------|
| 机房  | 光纤挖断   | 长         | 小，影响当前机房           | 低      |
|     | DDos攻击 |           |                    |        |
| 运营商 | 管控     | 难以预计      | 中，一般单运营商或者部分地区出现问题 | 中      |
|     | 出口异常   |           |                    |        |
| 云联网 | 路由下发异常 | 短，一般能快速恢复 | 大，整个region，甚至全国    | 高，一年多次 |
|     | 硬件升级异常 |           |                    |        |

# 多云接入落地

- 接入产品差异性可接受，可以通过标准化解决
- 完整流量调度体系减少网络故障影响
- 综合考虑，选择合适产品，必要时自己搭建



# 分享内容

---

1

云上流量接入现状

2

标准化，统一计费

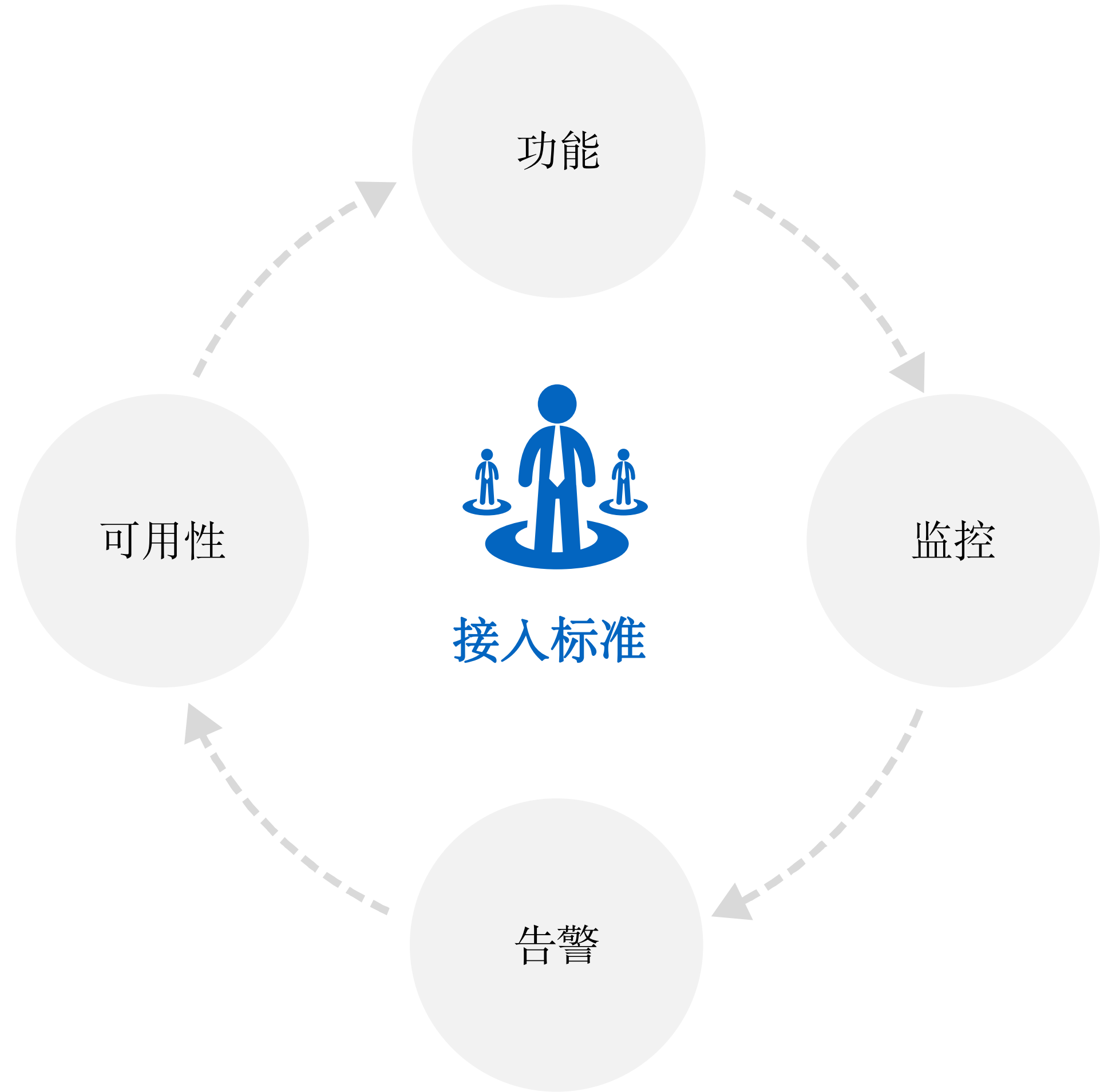
3

建立流量调度体系

4

多云收益最大化

# 基础接入标准



## 功能

功能列表，基础API能力基本一致，API对接，平台包装产品



## 监控

收集各个云的监控指标，统一单位和命名差异



## 告警

基于收集监控，提供多个云一致告警规则和内容



## 可用性

多可用区，多区域接入，资源充足

# 标准落地关键



# 核心产品标准

## DNS

就近解析  
内部多个k8s集群联动，打通微服务  
秒级解析生效  
基于标签进行流量调度



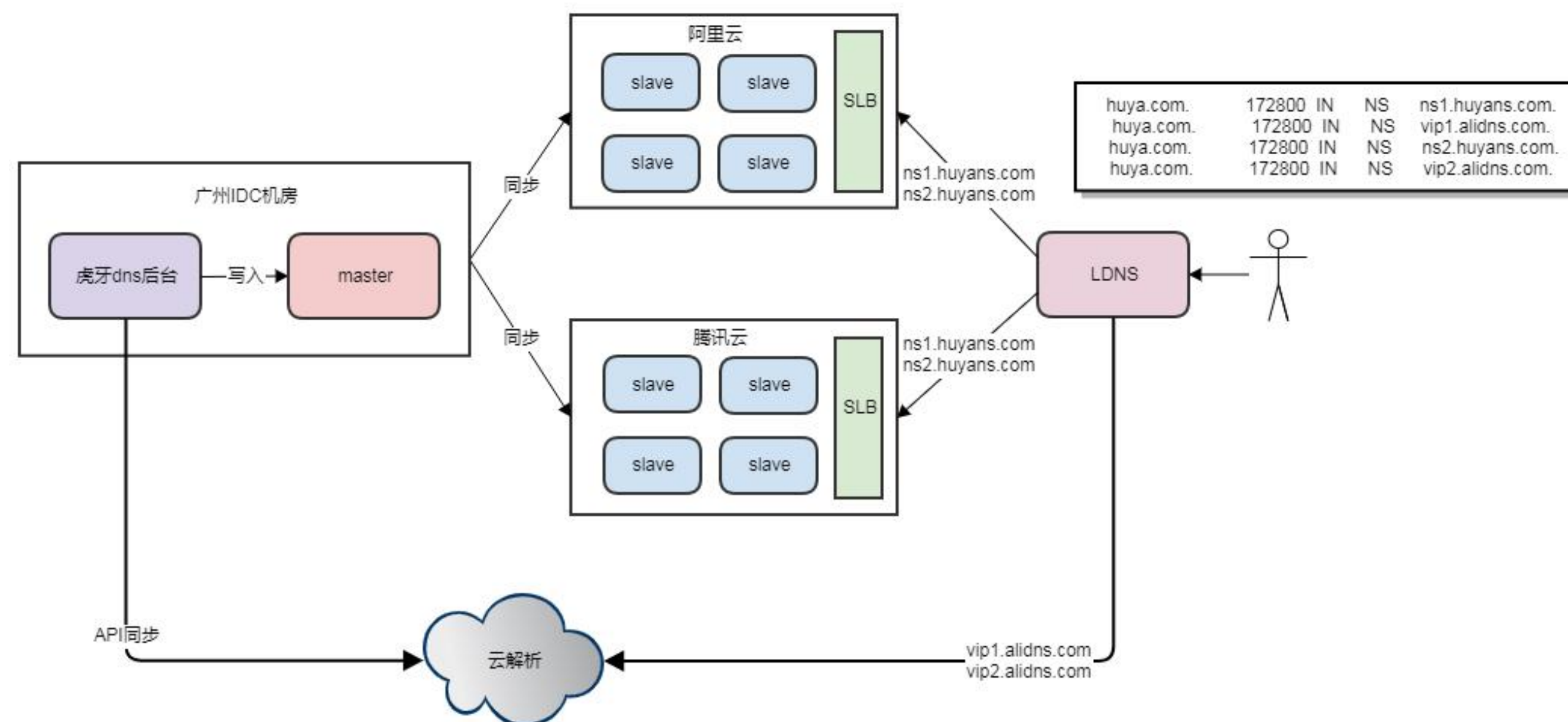
## 7层负载均衡

转发流量快速屏蔽  
证书安全需求  
基于域名和路径的监控指标  
灵活的扩展机制



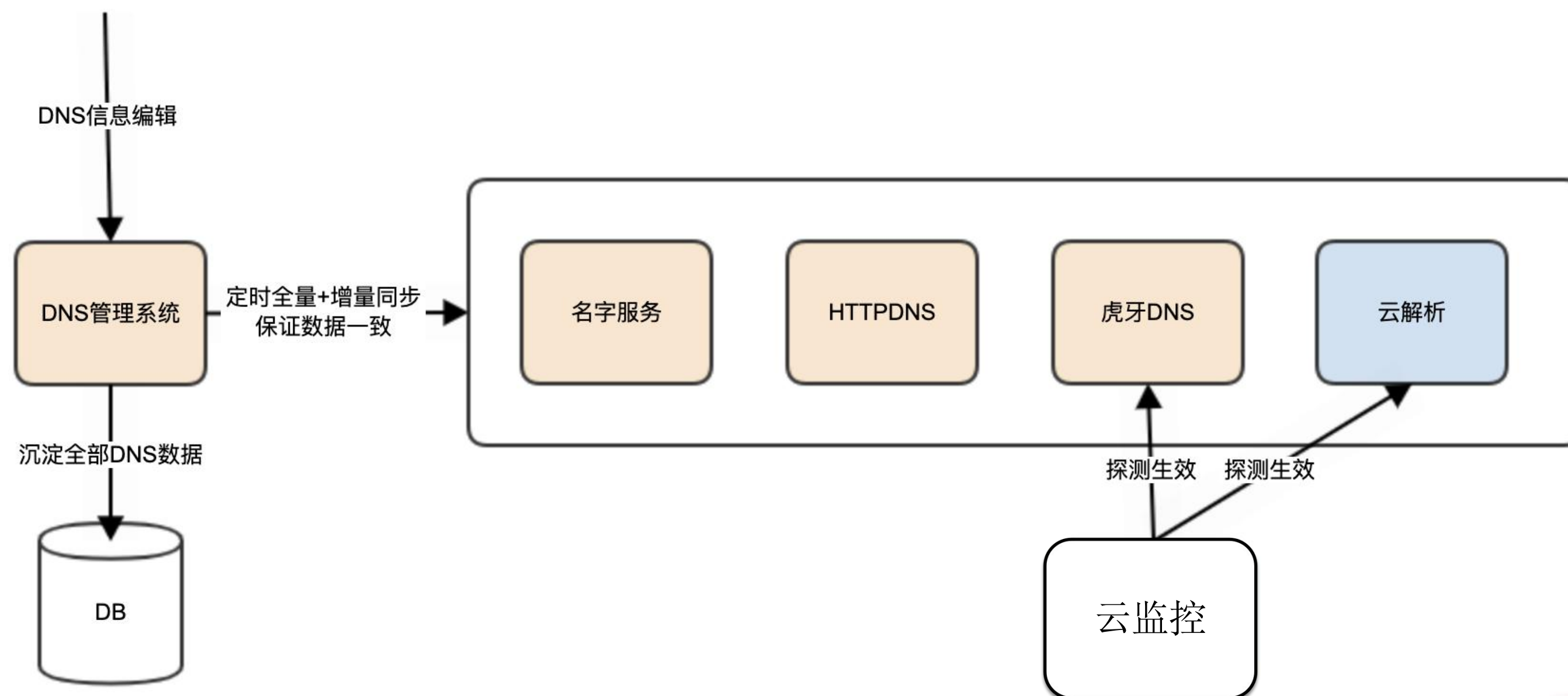
# 权威DNS

- 自建+云上解析同时使用
- 利用云上弹性资源部署slave节点
- 其中一个解析服务异常，可以自动切换



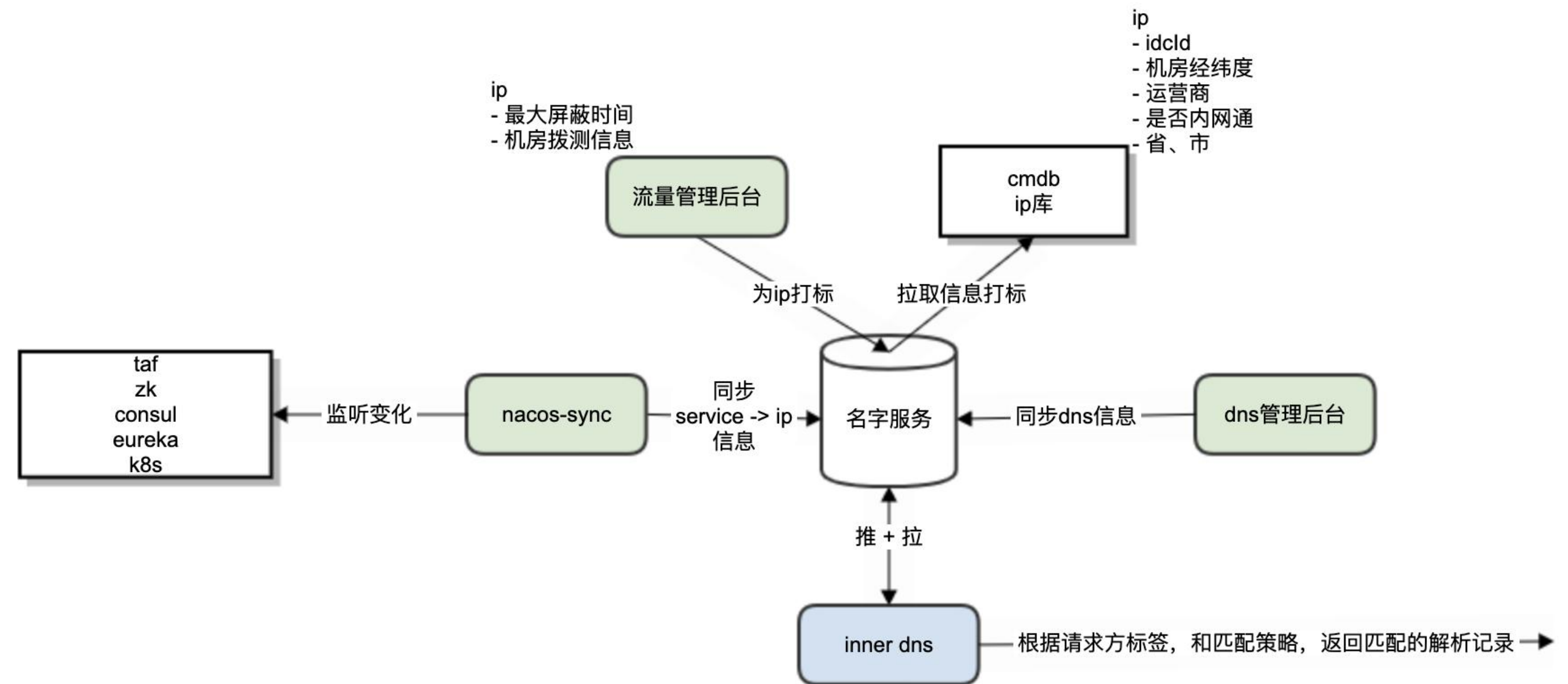
# DNS管理

- 统一的域名管理入口
- 全量+增量同步，保证一致
- 探测修改生效，监控生效时间



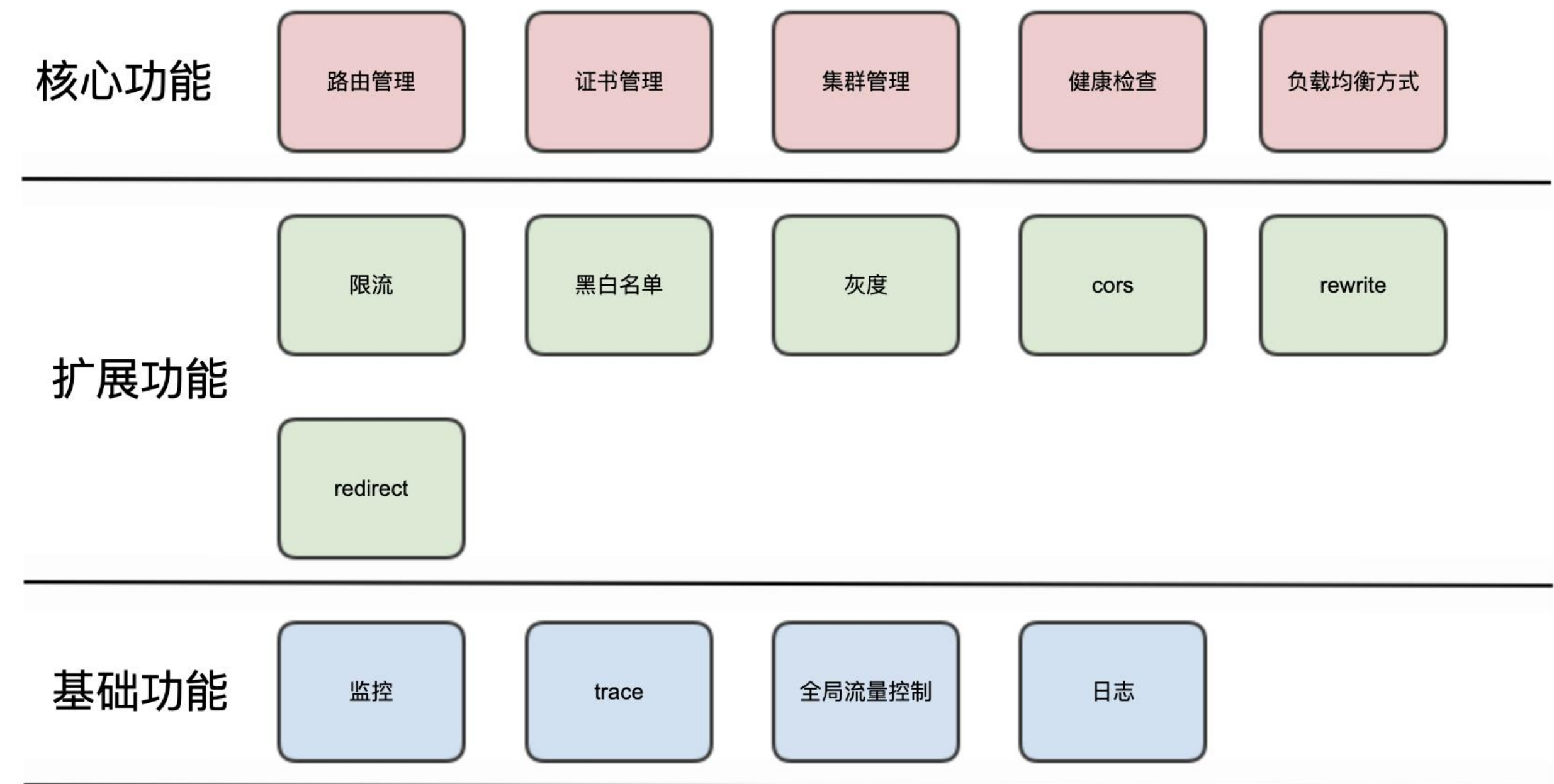
# 智能DNS

- 名字服务打通微服务、k8s集群、DNS信息，提供统一的内网DNS解析服务
- 基于标签和CMDB的信息，实现智能解析



# 7层负载均衡设计

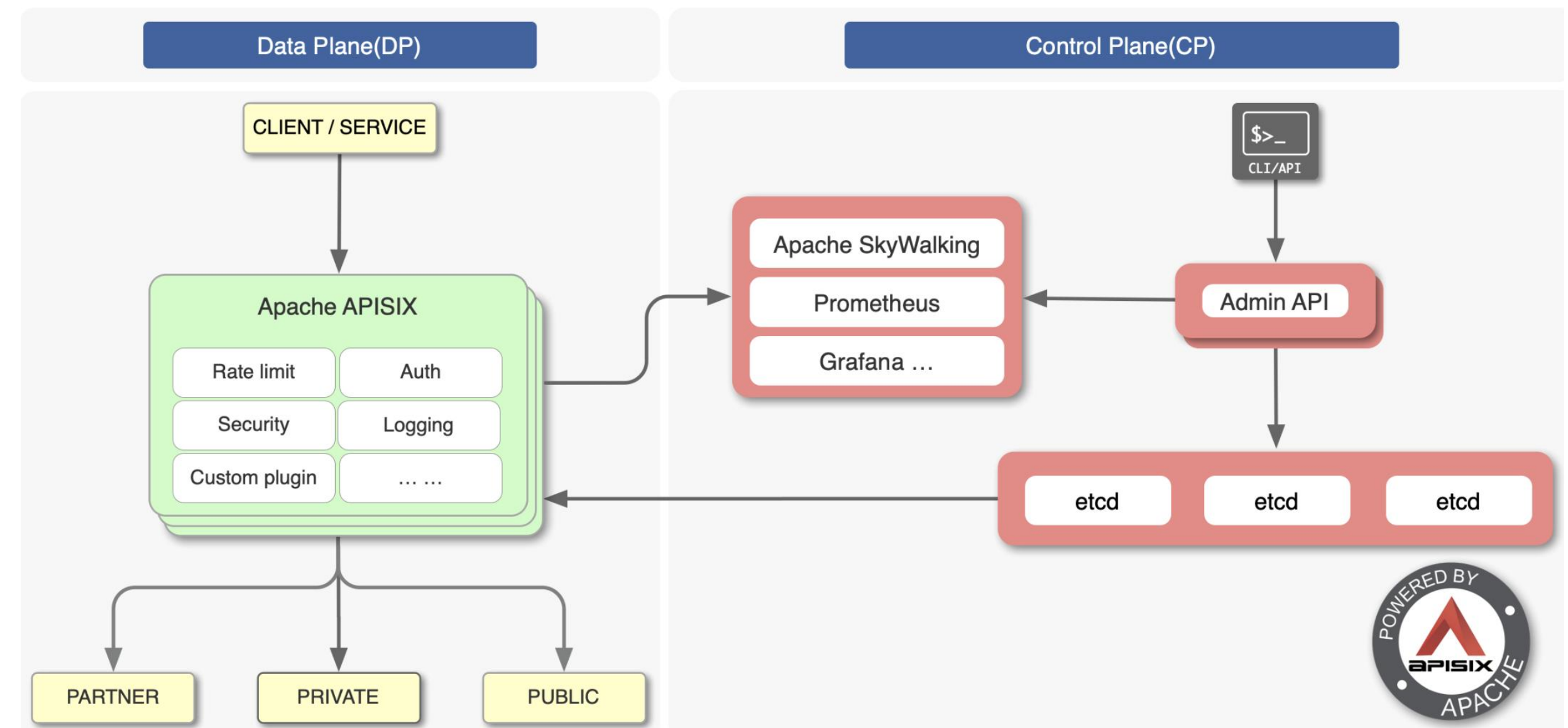
- 核心功能多云一致性，遵循统一规范
- 易于扩展，生效快速
- 基础功能符合开源标准，能与内部系统打通





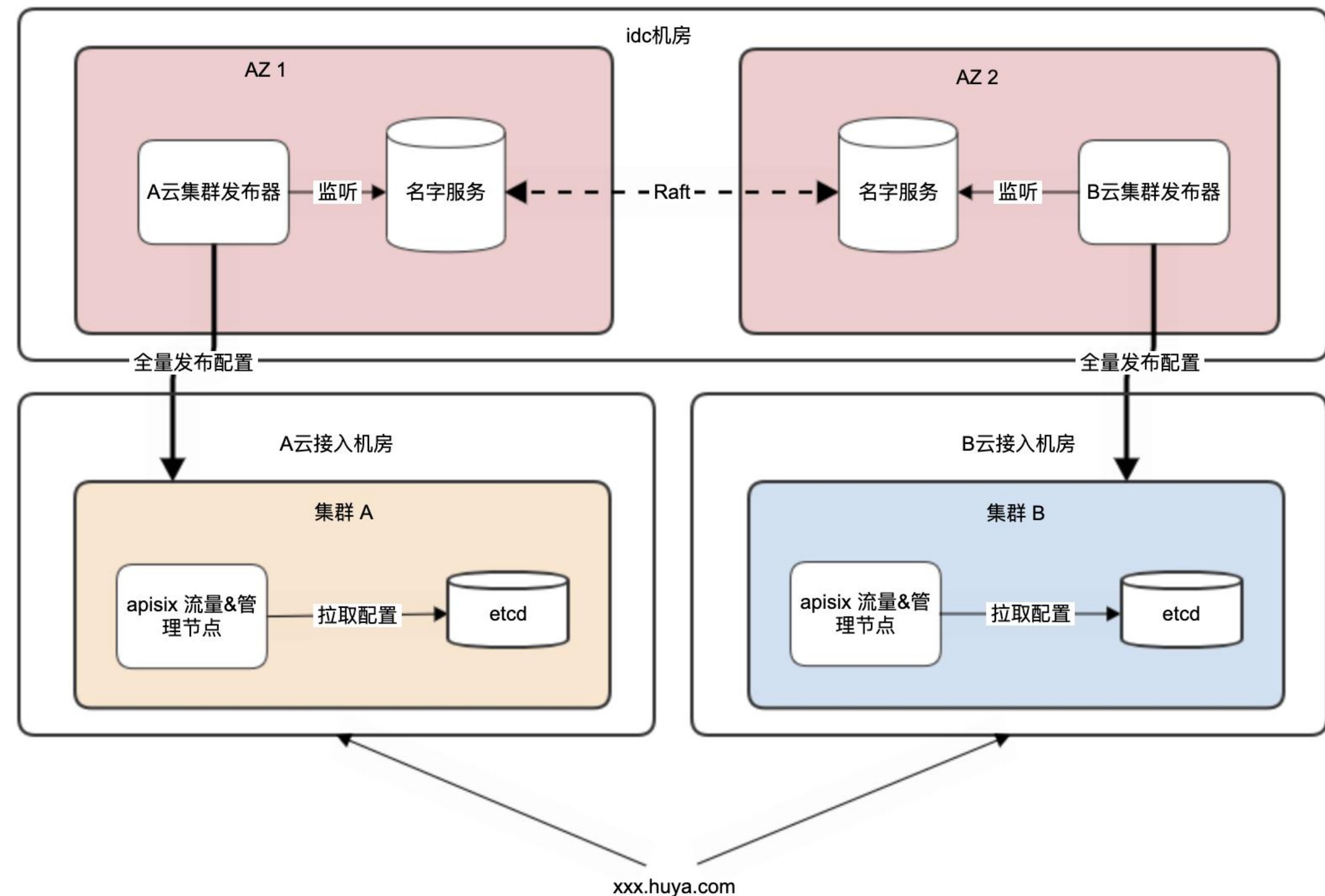
# 7层负载均衡选型

- 云上自建Apisix集群，不直接使用云上产品
- 基于Apisix插件的扩展机制，利用已有的插件，快速扩展
- 拥抱开源，实现标准，快速与内部系统打通



# 7层负载均衡部署

- 集群功能在单云，单区域闭环部署
- 域名维度配置全量增量更新，多云配置一致
- 日常各集群均分流量，网络问题，集群异常通过DNS屏蔽



# 控制成本

## 通过计费控制成本

建立统一计费能力，通过核心指标体现云厂商账单变化，以天为维度发现top成本



# 分享内容

---

1

云上流量接入现状

2

标准化，统一计费

3

建立流量调度体系

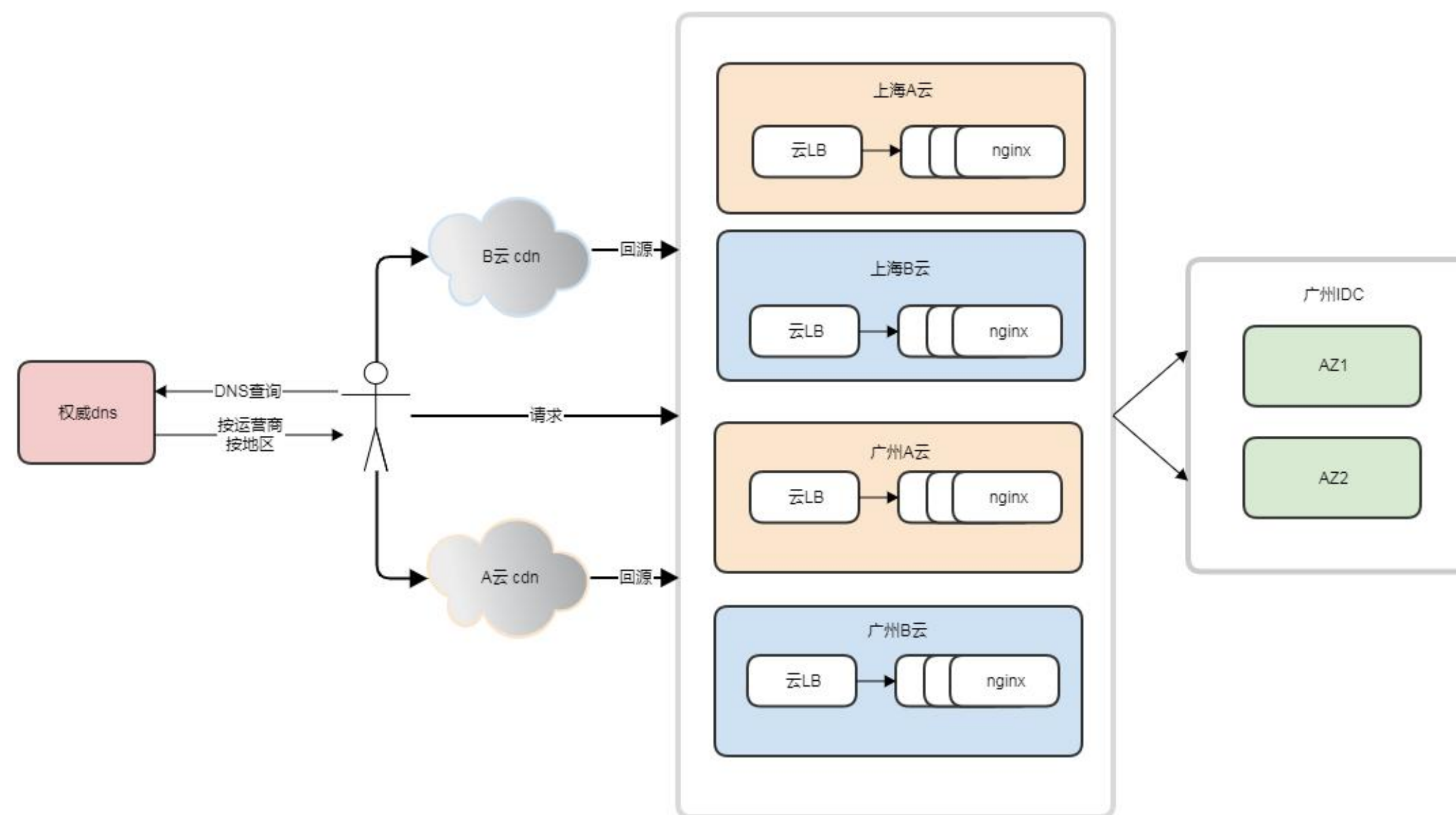
4

多云收益最大化



# 流量接入调度

- 多区域，多云接入点，公网DNS切换，5-10分钟生效
- 浏览器，客户端，CDN的重试，容错
- 能快速屏蔽转发到IDC机房单AZ流量



# DNS

## 就近解析

按照省、市，机房经纬度就近返回解析记录

## 快速生效

机房内域名解析秒级生效

## 运营商兜底策略

优先按照运营商匹配返回单线线路，无法识别的用BGP线路ip返回，进行兜底

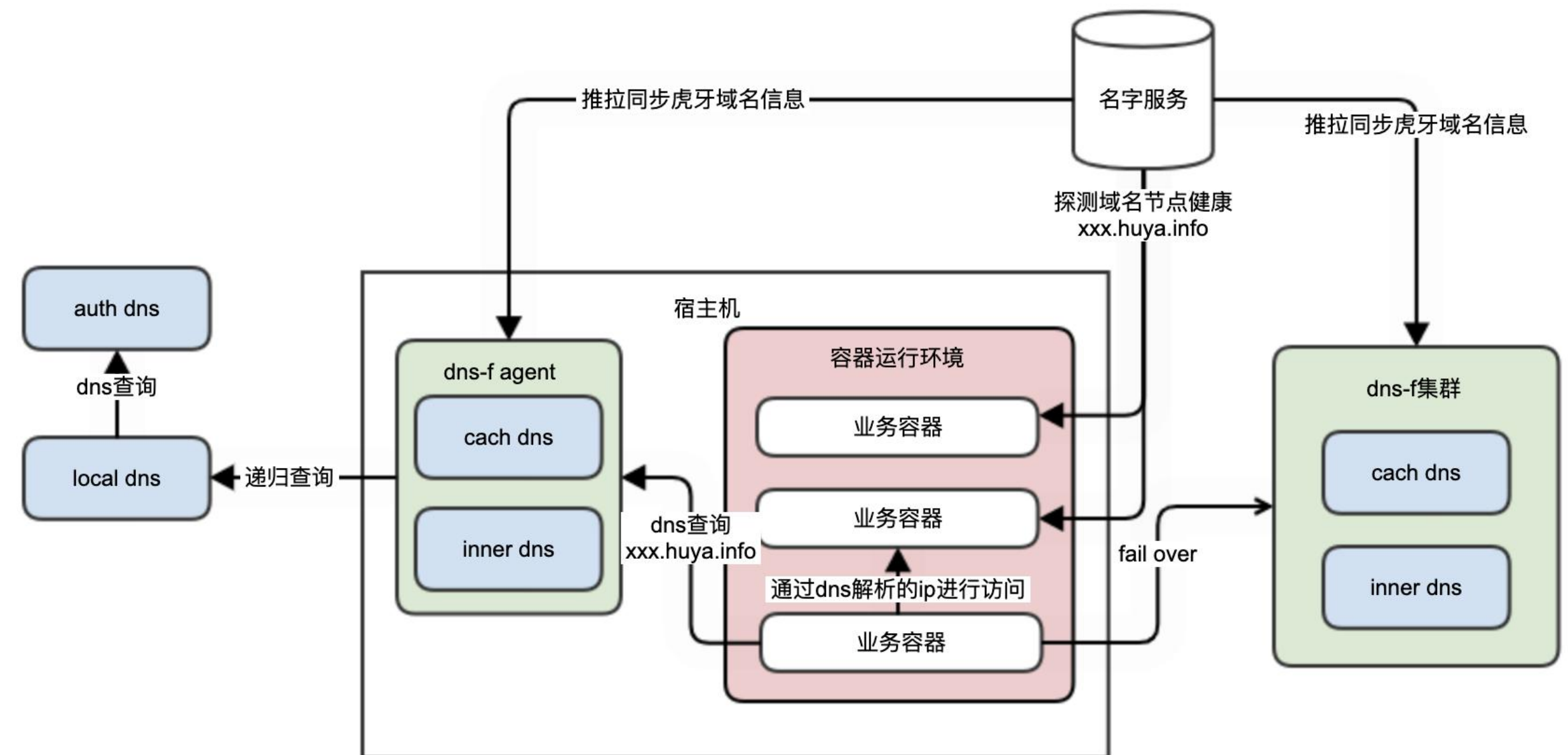
## 健康检查

对解析的ip进行探测，自动进行解析屏蔽



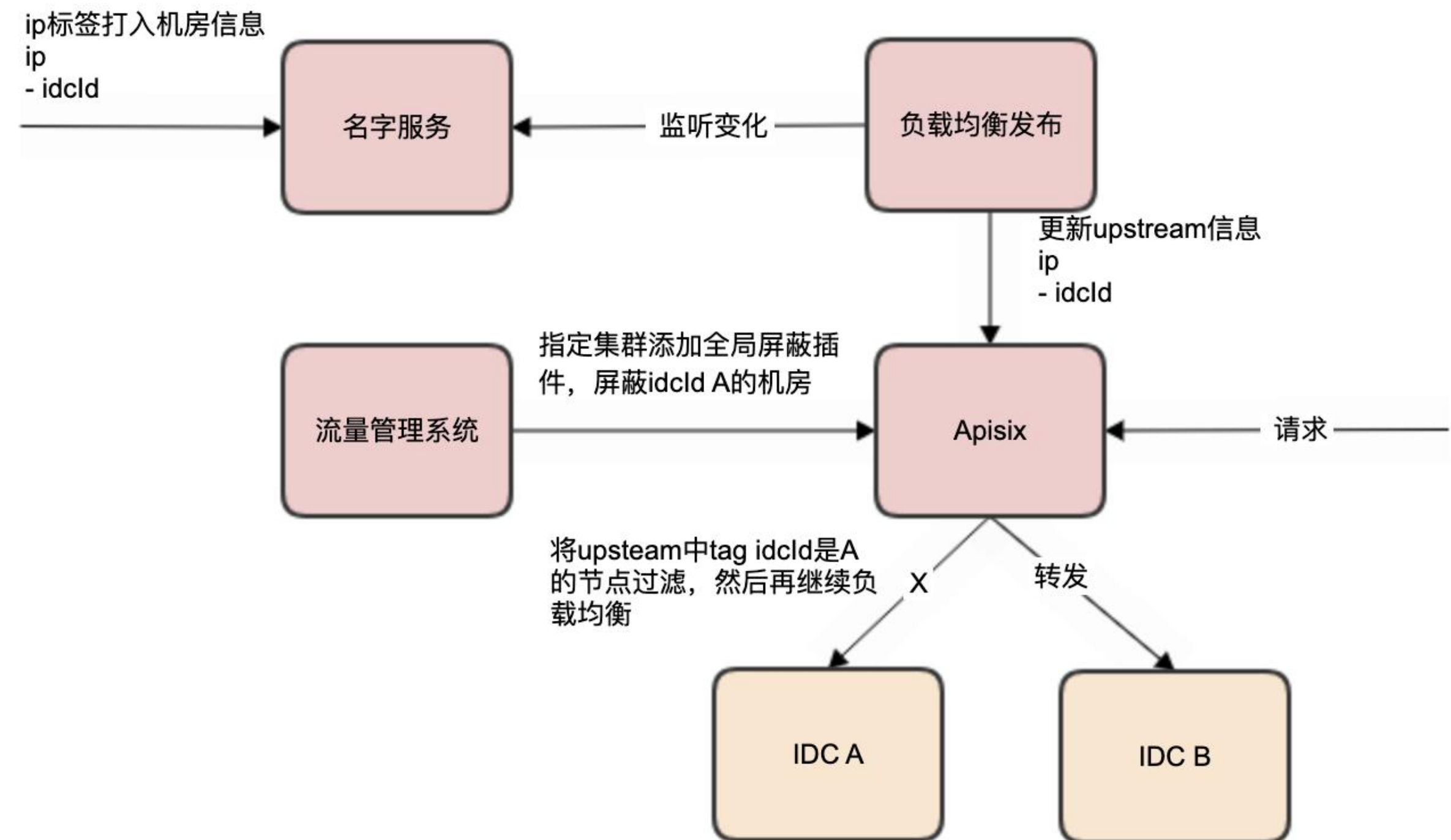
# 内部DNS快速生效

- 主机Agent劫持DNS解析，实时同步服务信息
- TTL默认为2秒，虎牙域名秒级生效
- 集成健康探测能力，快速节点屏蔽



# 7层流量转发调度

- 通过标签信息，在进行负载均衡前，将节点过滤
- 单个指令操作，集群级快速生效，不需要逐个域名进行配置，秒级快速生效





# 分享内容

---

1

云上流量接入现状

2

标准化，统一计费

3

建立流量调度体系

4

多云收益最大化

# 多云接入收益

## 成本

利用二线城市单线带宽，成本降低50%

IDC机房减少80%buffer机器，高峰期云上扩容



## 高可用

保护IDC机房，云上每年5-10次的攻击事件，IDC机房没有发生

单云，单区域异常，公网5分钟内切换，内网10s内生效



## 效率

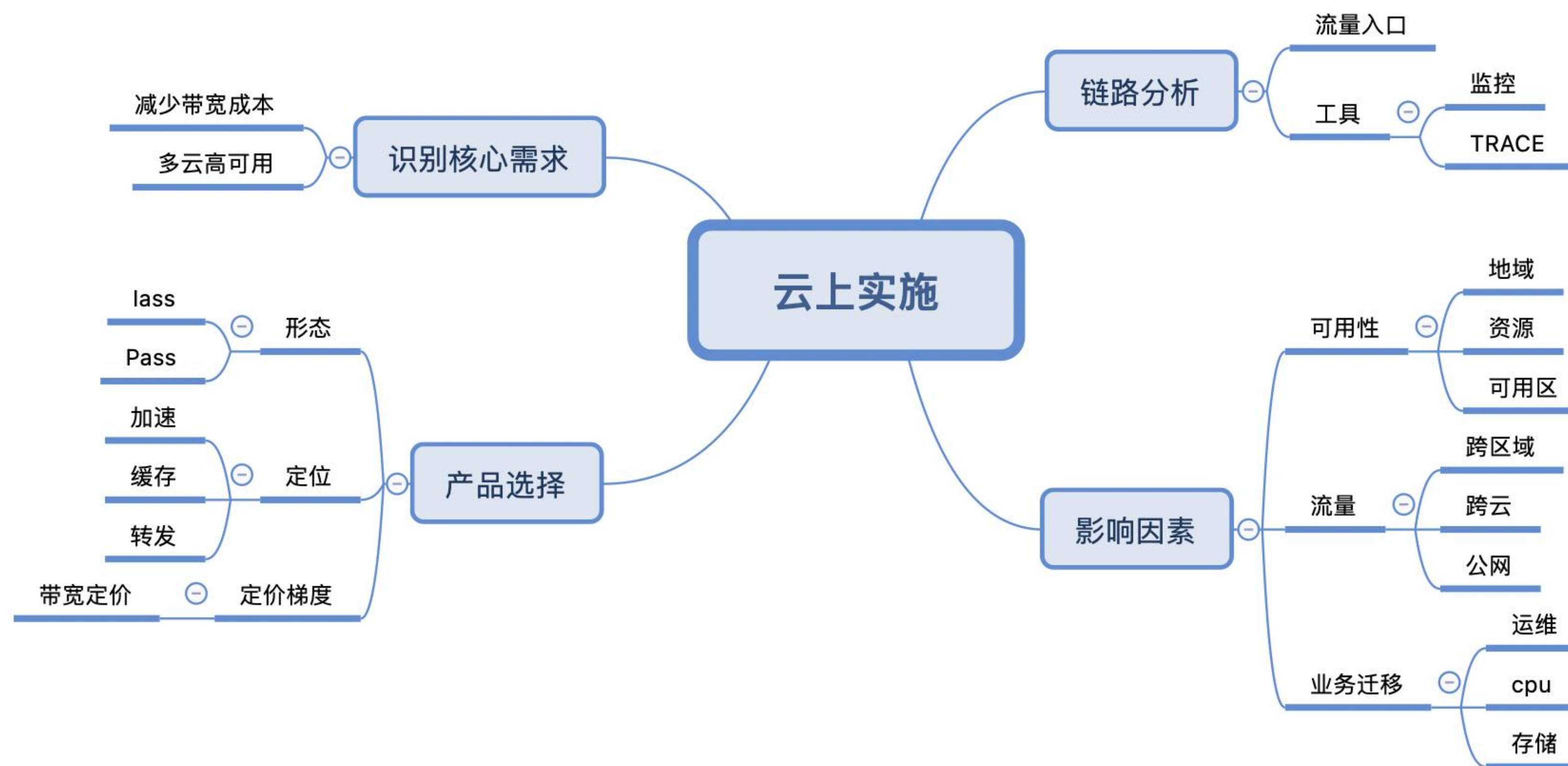
分钟级完成1000core，支撑20Gb带宽的接入层扩容

运维人力成本减少3-4人

新云厂商接1周完成



# 多云接入实施思路



# 安全产品选择

- 保证核心比赛期间的安全稳定
- web请求复杂，性能敏感
- 按需使用，低改造成本
- 漏洞实时阻断的要求低



# 安全产品选择

|        | 产品模式 | 特点                | 性能损耗 | 方案考虑              |
|--------|------|-------------------|------|-------------------|
| DDos高防 | 全力防护 | 使用原ip，防护能力与当前机房相关 | 低    | 改造成本低，防护能力足够      |
|        | 高防ip | 使用前置代理，需要更换为高防ip， | 低    | 需要改变访问链路          |
| Waf    | 反向代理 | 实时分析，及时阻断         | 高    | 需要改变访问链路，并不需要实时阻断 |
|        | 旁路分析 | 只分析，不阻断           | 无    | 作为数据来源，用内部安全分析    |

# 安全产品选择

## 选择

平日使用5Gb基础防护

S赛购买全力防护

旁路分析+定期漏洞扫描



## 收益

有一定防护能力，控制成本，必要时屏蔽异常节点

保证核心业务正常，不需要额外改造成本

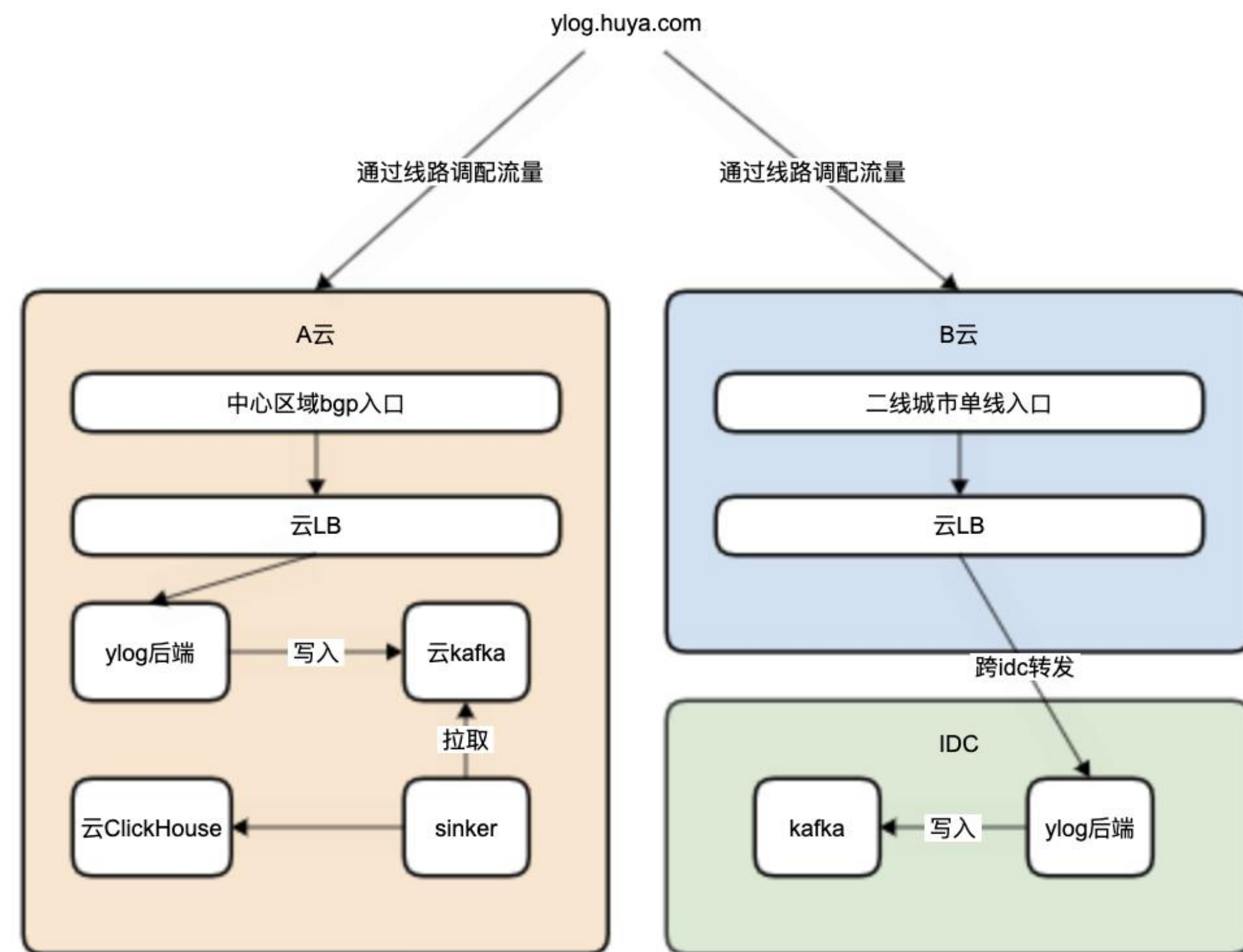
事后修复漏洞，屏蔽攻击源

# 降低指标上报成本

- 用户操作，音视频，网络等指标
- 带宽峰值20Gb+， 成本敏感， 有弹性需求
- 上下游依赖多
- 功能单一， 没有太多扩展需求

# 降低指标上报成本

- 利用低成本带宽，IDC闭环处理
- 流量在云上闭环，利用云上弹性资源和低运维服务
- 同时运行两套方案，流量调配，按需控制成本





# THANKS



—  
软件正在重新定义世界

Software Is Redefining The World